



UNCLASSIFIED



North Dakota Homeland Security Anti-Terrorism Summary



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

[Government Sector \(including Schools
and Universities\)](#)

[International](#)

[Information Technology and
Telecommunications](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials
Sector](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Commercial Facilities](#)

[Public Health](#)

[Communications Sector](#)

[Transportation](#)

[Critical Manufacturing](#)

[Water and Dams](#)

[Defense Industrial Base Sector](#)

[North Dakota Homeland Security
Contacts](#)

[Emergency Services](#)

NORTH DAKOTA

Pressure eases on dam, residents in ND town. The Des Lacs River's slow decline took the pressure off a fragile dam and the people who live nearest it, with most of the evacuees in a 30-home development in Burlington, North Dakota, filtering back home to turn their attention to cleanup and flooded basements. The fire chief said the neighborhood was not in the clear yet, but cooler weather had slowed runoff from snow lingering in the area, leaving him optimistic. Just 2 days after an estimated 25 of the houses had been evacuated, he said all but 5 to 10 homeowners had returned. Water levels had fallen more than a foot and the river had retreated from overflowed banks by about 3 feet compared with a day earlier, state and local officials said. Water behind the troubled Burlington Dam No. 1 was down by about a half-foot, and the dam was holding steady, said North Dakota's state engineer. Flooding fears eased elsewhere in North Dakota, too. A 30-mile stretch of Interstate 29 reopened north of Fargo after being closed by overland flooding, and to Fargo's west, officials said Valley City appeared poised to escape flooding from the Sheyenne River after raising its levees. In Burlington, the strength of the 77-year-old dam has been suspect for decades, but this year's flooding has spurred a need to either repair the dam or intentionally breach it by next spring, the engineer said. For now, authorities are watching the ailing structure with remote video cameras, fearing any attempt to shore up the dam — or even walk across it — could cause it to collapse. About 1,200 people live in Burlington. Those in most immediate danger are on the west edge of town, and he said the risk to the rest of the city was "very, very minimal." Source:

<http://www.greenwichtime.com/news/article/Pressure-eases-on-dam-residents-in-ND-town-1338519.php>

More of I-29 closed in ND because of flooding. Officials prepared to close another section of Interstate 29 in eastern North Dakota April 13 because of flooding. The state transportation department said a 28-mile section between Manville and Grafton would be closed to everything but emergency vehicles and commercial trucks of at least 26,000 pounds. A 30-mile stretch of I-29 north of Fargo remains closed as well. The transportation department said that section could be closed for a few days while it is checked for erosion and washouts beside or beneath the roadway. Source:

<http://www.devilslakejournal.com/newsnow/x1225322055/More-of-I-29-closed-in-ND-because-of-flooding>

In N. Dakota, flood attention turns to rural areas. Residents in North Dakota's most populous county were finding new ways to get around April 11 as floodwaters put two small towns "under siege" and closed more than 60 miles of county roads. The state's governor was caught in rural traffic detoured by flooded roads. The north-flowing Red River crested in Fargo and neighboring Moorhead, Minnesota, over the weekend of April 9 and 10 at 38.75 feet, the fourth-highest flood on record. Officials said the levees were holding in the two cities, and offered to help with unprecedented flooding in Cass County directly north of Fargo. The largely rural territory is dotted with small towns, many with just a few hundred residents, and a National Weather Service meteorologist said record flows in the Sheyenne, Maple, and Rush rivers led to unparalleled overland flooding. Road closures

UNCLASSIFIED

were making life difficult for county residents, including commuters who normally use Interstate 29 to get to work in Fargo. More than 30 miles of the interstate remained shut down from north of Fargo to Hillsboro. State transportation officials said roads that have never flooded before are now under water. A handful of people were rescued April 10 in Cass County, and county and U.S. Coast Guard air boats were on standby April 11, but no new evacuations were reported. USCG officials said they suspended routine checks on flooded properties because of the fear the wave action could damage levees. Work was being done April 11 to reinforce levees in the Minnesota towns of Perley, Halstad, and Hendrum. It was less hectic in Fargo and Moorhead. Fargo was removing clay levees and opening bridges that cross drainage areas. Source:

<http://www.grandforksherald.com/event/apArticle/id/D9MHO7I82>

2 ND dams monitored closely this flooding season. Authorities are keeping a close eye on two dams in North Dakota. A Burlington police officer told KCJB radio the Horse Shoe Dam on the Des Lacs River was being bolstered after officials discovered it had holes. He said rural residents near the river were being urged to leave. And in southeast North Dakota, the state water commission told The Forum newspaper repairs to the Clausen Springs Dam near Kathryn were holding up well despite high water in the reservoir. Source: <http://www.wday.com/event/article/id/45874/group/homepage/>

Companies say ND wind turbine accident unique. Experts said a North Dakota wind turbine's rotor and blades crashed to the ground because they were not properly aligned with a power shaft atop the turbine's steel tower, which caused the rotor's connecting bolts to fail. The March 14 incident north of Rugby will prompt more frequent inspections of other turbines, said the director of wind plant engineering for Iberdrola Renewables Inc. of Portland, Oregon. The director told North Dakota's Public Service Commission that investigators were unsure whether the problem resulted from the turbine's operation or reflected an assembly flaw. He said the incident was "very out of the ordinary" and "a singular event" that did not indicate a broader problem. The turbine was one of 71 that make up an Iberdrola wind energy project in Pierce County, which is capable of generating 149 megawatts of power. Source: http://www.forbes.com/feeds/ap/2011/04/12/business-us-nd-wind-blades-fall_8403852.html

Ammonia leak reported at elevator in Horace. Residents in Horace, North Dakota, received a scare April 9 when they were forced to take shelter in their homes after an anhydrous ammonia leak was reported south of town. The leak occurred at the Harvest States Elevator just before 10 a.m. and was contained around 10:40 a.m. Emergency responders had to transfer 30,000 gallons of anhydrous ammonia from the leaking tank to a good tank to get it under control, a Cass County administrator said. A small ammonia cloud was visible but dissipated after a short while, officials said. A 1-mile perimeter was set up around the city. The public was asked to stay away from Horace, and residents were asked to stay inside their homes for several hours. Residents were notified of the danger with a CodeRED call. Officials did not evacuate the area because that would have put people in contact with the chemical, the administrator said. Source:

<http://www.inforum.com/event/article/id/315548/group/News/>

REGIONAL

(Minnesota) Edina woman linked to \$3.65 billion ponzi scheme pleads guilty. A 43-year-old Edina, Minnesota woman pleaded guilty April 8, in federal court to playing a role in a \$3.65 billion Ponzi

UNCLASSIFIED

UNCLASSIFIED

scheme. The woman admitted she aided and abetted criminal activity by concealing information from investors regarding the purchase and sale of securities from September 2007 through September 2008. She entered a guilty plea to one count of securities fraud and one count of providing false statements to a government agent before a U.S. district court judge. The woman served as vice president of special operations and later as managing director of finance with Arrowhead Management, which operated three hedge funds that almost exclusively invested in Petters Company, Inc. (PCI) promissory notes. The man who owned and operated PCI was sentenced to 50 years in federal prison in April 2010 for heading up the scheme. The woman admitted in court she and others hid information from investors that millions of dollars in PCI notes held by Arrowhead were on the verge of going into default. During the life of the hedge fund, investors reportedly contributed more than \$387 million, with Arrowhead obtaining about \$35 million in fees from the fund. She faces a potential maximum penalty of 5 years in prison for each charge. Source:

<http://edina.patch.com/articles/edina-woman-linked-to-365-billion-ponzi-scheme-pleads-guilty>

(South Dakota) S.D. corrections officer killed during escape attempt. Two convicted kidnappers killed a 63-year-old prison guard April 12 during a failed attempt to escape from a Sioux Falls, South Dakota prison where they were serving lengthy sentences, authorities said. The two convicts were apprehended on the grounds of the South Dakota Penitentiary, and a sweep of the facility showed all staff and inmates were accounted for, the state department of corrections said. The duo tried to escape shortly before 11 a.m., assaulting the guard in the process, the department of corrections said. The corrections officer who had worked at the penitentiary for more than 23 years was pronounced dead at a hospital, and a second guard suffered minor injuries. The department did not release further details about the escape attempt or attack. The prison, which has both maximum and minimum security wings, was locked down pending an investigation. The two convicts were taken to the county jail in Sioux Falls, authorities said. Source: <http://www.officer.com/news/10254036/sd-corrections-officer-killed-during-escape-attempt>

NATIONAL

Mexican security forces arrest 2 men carrying grenades. Two men were arrested by Mexican police and army troops as they picked up two suitcases packed with grenades that were passed to them in Baja California state from the U.S. side of the border, officials said. The suspects were arrested April 11 when they were spotted by a patrol, 2nd Military Region commander general, the Duarte and Mexicali municipal police chief said in a press conference. The arrests were made near border post Number 2 in Mexicali, the capital of Baja California. The two suspects tried to escape, but they were apprehended, the police chief said. The suitcases contained 194 grenades of different types, 192 fuses and 3 boxes with parts for different types of weapons, including AR-15 rifles, the police chief also stated. Investigators suspect the grenades, which are similar to those used in a recent attack on a bar in Guadalajara, the capital of the western state of Jalisco, were bound for central Mexico. Source: <http://latino.foxnews.com/latino/news/2011/04/13/mexican-security-forces-arrest-2-men-carrying-grenades/>

INTERNATIONAL

Somali pirates zero in on oil tanker lanes. Somali pirates are increasingly threatening global oil supplies from the Persian Gulf as they extend their attacks ever deeper into the Arabian Sea and

UNCLASSIFIED

Indian Ocean, morphing from a tactical nuisance to a strategic danger. Three supertankers have been seized so far in 2011, the first time since the piracy plague began in 2006 that so many have been captured in a three-month period. The International Maritime Bureau in London, which monitors international shipping, reports piracy hit an all-time high in the first quarter of 2011 with 142 attacks worldwide, mostly by Somali sea bandits. Of the 97 attacks pinned on Somali pirates — up from 35 in the equivalent period in 2010 — 37 were on tankers, including 20 with a deadweight of more than 100,000 tons, the bureau said. The “dramatic increase in the violence and the techniques” employed by the Somali marauders put large tankers carrying oil or inflammable chemicals at serious risk, a spokesman stressed. As the pirates increasingly concentrate their attacks close to the Persian Gulf, calls are mounting for tougher action against the marauders. The piracy problem “is spinning out of control into the entire Indian Ocean,” the managing director of the International Association of Independent Tanker Owners said February 9. “If piracy in the Indian Ocean is left unabated, it will strangle these crucial shipping lanes with the potential to severely disrupt oil flows to the United States and the rest of the world,” he said. Source: http://www.upi.com/Science_News/Resource-Wars/2011/04/14/Somali-pirates-zero-in-on-oil-tanker-lanes/UPI-35161302806016/

Tijuana police make arrest in U.S. agent’s killing. Police in Tijuana, Mexico, said April 11 that officers arrested a man suspected of killing a U.S. Border Patrol agent near San Diego, California nearly one year after another person was sentenced to prison for his role in the ambush. The suspect was taken into custody as he was driving through Tijuana aided by information provided by the FBI, said Tijuana’s police director. Mexico’s federal attorney general’s office had issued an arrest warrant for the Tijuana native on suspicion of killing a Border Patrol agent, who died during an attempted robbery in the mountains east of San Diego in July 2009. An additional suspect, who was 16 at the time of the killing, pleaded guilty to murder in San Diego for his role in the killing and was sentenced last April to 40 years in prison. His attorney said before sentencing that two collaborators were in Mexico. Source: <http://www.foxnews.com/us/2011/04/11/tijuana-police-make-arrest-agents-killing/?test=latestnews>

Belarus hunts bombers as 12 die in Minsk subway explosion. Belarus ordered a security crackdown after at least 12 people died and 149 were wounded in a subway bombing that authorities classified as the first terrorist attack since the current president came to power in 1994. The explosive device went off during evening rush hour April 11 at the capital Minsk’s, busiest metro station, which is near the presidential residence, according to the Belarusian security agency. The president ordered security tightened “to the uttermost” and said the blast may have been orchestrated from abroad, according to a transcript of an emergency government meeting published on the president’s Web site late April 11. The prosecutor general’s office declared the blast “an act of terrorism” and began a criminal investigation, Belarusian state television said. Authorities detained three people in connection with the explosion, including one suspect, a KGB chairman said, according to state-run news agency Belta. The chairman said law-enforcement authorities prepared a composite sketch of an alleged attacker, a 27-year-old man of non-Slavic appearance. The KGB chief added that the bomb had been radio-controlled. No one has yet claimed responsibility for the attack. The device went off as two trains were arriving at the Oktyabrskaya station, where the capital’s two metro lines intersect, the interior minister told his president at their meeting. The bomb, which was equivalent to 5 to 7 kilograms of TNT, left a crater 31 inches deep, he said. Source: <http://www.businessweek.com/news/2011-04-12/belarus-hunts-bombers-as-12-die-in-minsk-subway-explosion.html>

Dutch mall shooter fired more than 100 times. Dutch prosecutors said the man who went on a shooting rampage in a Netherlands mall April 9 fired more than 100 rounds in a few minutes as he killed 6 shoppers before turning one of his weapons on himself. Prosecutors said the 24-year-old used three different guns during the shooting spree April 9 at the busy Ridderhof mall in the central city of Alphen aan den Rijn. Prosecutors released details of the shooting April 11 after studying video images from mall security cameras. The gunman shot one man before entering the mall, and then walked back and forth shooting from three guns. He had permits for all three. Detectives are still investigating whether one of the guns, a semiautomatic, had been illegally modified to turn it into a fully automatic weapon. Source: http://www.forbes.com/feeds/ap/2011/04/11/general-eu-netherlands-mall-shooting_8401501.html

BANKING AND FINANCE INDUSTRY

Exploit-wielding boffins go on free online shopping binge. Computer scientists have documented serious flaws in software running some of the world's biggest e-commerce sites and shown how they can be exploited to receive DVDs, digital journals, and other products for free or at sharply reduced prices not authorized by sellers. The findings are an indictment of software makers, e-commerce sites, and third-party cashiers used to process payments. The researchers, from Microsoft and Indiana University, said the vulnerabilities stem from the interconnected communication among the end user making a purchase, the online merchants, and the cashier-as-a-service providers such as PayPal, Amazon Payments, and Google Checkout. The "trilateral interaction" is so complex the two most popular e-commerce programs used to coordinate the communications can easily be fooled into approving the transactions for free, or at a tiny fraction of the price being charged. They said the software they analyzed was vulnerable largely because it was designed to be flexible enough to work with a variety of merchants and payment processors. But they said the payment processors were also culpable. They called out Amazon Payments specifically for a "serious error" in its software developer kit that allowed attackers to provide their own digital certificates during online transactions so they bypassed legitimate certificates used during a verification process. Source: http://www.theregister.co.uk/2011/04/12/free_online_shopping_exploits/

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

(Arizona) Man arrested in bomb scare at Arizona nuclear plant. A contractor arriving for work at the nation's largest nuclear plant was arrested April 15 after suggesting he had a bomb in his car, authorities said. The man is in custody after causing a roughly 5-hour lockdown of the Palo Verde Nuclear Generating Station in Wintersburg, Arizona, a Maricopa County Sheriff's Office spokesman said. "Our bomb squad has just cleared the vehicle and no explosives were found," he told Reuters. "There was no danger to the plant. Everything is fine." He told Reuters the man faces possible felony charges. Authorities said the man was undergoing a routine inspection at about 12:45 a.m. and made an "off-handed remark" that he had a bomb in his car. Sheriff's deputies were called and no one was allowed in or out of the plant. The spokesman said the gate is about 1,000 feet from any plant operations. Source: <http://www.publicbroadcasting.net/wbfo/news.newsmain/article/0/0/1789669/US/Man.arrested.in.bomb.scare.at.Arizona.nuclear.plant>

UNCLASSIFIED

EPA concerned with two consumer chemicals. The U.S. Environmental Protection Agency (EPA) said it will take action on potential health risks of two chemicals consumers may encounter in construction products. Methylene diphenyl diisocyanate, toluene diisocyanate, and related compounds are used in certain applications such as spray foam insulation, sealing concrete, or finishing floors, an EPA release said April 13. "There has been an increase in recent years in promoting the use of foams and sealants by do-it-yourself energy-conscious homeowners, and many people may now be unknowingly exposed to risks from these chemicals," said the assistant administrator for EPA's Office of Chemical Safety and Pollution Prevention. Diisocyanates are known to cause severe skin and breathing responses in workers who have been repeatedly exposed to them, EPA said, and have been documented as a leading cause of work-related asthma. In severe cases, fatal reactions have occurred, the agency said. Actions contemplated by EPA include requiring exposure monitoring studies for consumer products, improved labeling and product safety information, and if necessary possibly banning or restricting consumer products containing uncured MDI or TD. Source: http://www.upi.com/Science_News/2011/04/13/EPA-concerned-with-two-consumer-chemicals/UPI-47831302733493/

Japan to raise Fukushima crisis level to worst. The Japanese government's nuclear safety agency has decided to raise the crisis level of the Fukushima Daiichi power plant accident from 5 to 7, the worst on the International Nuclear and Radiological Event Scale (INES). The nuclear and industrial safety agency made the decision April 11. It said the damaged facilities have been releasing a massive amount of radioactive substances that are posing a threat to human health and the environment over a wide area. INES was designed by an international group of experts to indicate the significance of nuclear events with ratings of 0 to 7. On March 18, 1 week after the massive earthquake and tsunami, the agency declared the Fukushima trouble a level 5 incident, the same as the accident at Three Mile Island in the United States in 1979. Level 7 has formerly only been applied to the Chernobyl accident in the former Soviet Union in 1986 when hundreds of thousands of terabecquerels of radioactive iodine-131 were released into the air. One terabecquerel is 1 trillion becquerels. The agency believes the cumulative amount from the Fukushima plant is less than that from Chernobyl. Officials from the agency and Japan's nuclear safety commission were scheduled to discuss the change of evaluation at an April 12 news conference. Source: http://www3.nhk.or.jp/daily/english/12_05.html

COMMERCIAL FACILITIES

Nothing Significant to Report

COMMUNICATIONS SECTOR

DDoS attacks grow in sophistication. In the wake of the attacks by the hacker collective Anonymous on Sony and on Livejournal, more attention has been focused on just what such attacks mean and how to defend against them. Most attacks on the Web come as distributed denial of service attacks, or (DDoS). The most common form is making too many requests of a server for it to handle at once. By flooding a server with data packets, one can essentially shut it down, making it inaccessible to other users. To set one up requires a large number of computers, and a simple way to do it is to send out a piece of software — usually a virus or Trojan to unsuspecting users whose computers mount the attack without them knowing. Such a network is called a botnet. Another method is to enlist the help of others voluntarily. The Low Orbit Ion Cannon (LOIC) is a piece of software that can target a

UNCLASSIFIED

Web site but it has to be run by a user helping mount a DDoS. LOIC was originally a stress-testing tool for system administrators. Such attacks are not too difficult to defend against, a director of security products at Radware said. That is because any attack that depends on simply sending lots of data can be stopped if certain Internet addresses are blacklisted, or if the target can remove some of the packets from the stream of data. By having in place a piece of hardware or software that takes some packets out, the server is convinced there is a congestion problem, and it reduces the amount of data sent in and out. That can defeat the DDoS. Source:

<http://www.ibtimes.com/articles/132456/20110409/ddos-attacks-the-arms-race.htm>

CRITICAL MANUFACTURING

Ford recalling 1.2 million F-150 pickups. Under pressure from government regulators, Ford Motor Co. is expanding a recall of the popular F-150 pickup truck to include nearly 1.2 million vehicles that may have defective air bags. The additional recall, announced April 14 by the National Highway Traffic Safety Administration (NHTSA), covers trucks from the 2004 through 2006 model years. An electrical short can cause the air bags to deploy unexpectedly, in some cases injuring drivers. In February, Ford agreed to fix 150,000 of the trucks but resisted the government's wishes to recall all 1.2 million trucks that may have the problem. Ford's F-Series pickup truck is the top-selling vehicle in America, and the F-150 makes up about 60 percent of F-Series sales. The Dearborn, Michigan company said in a statement that it will notify all owners in May that they should take their trucks to a dealer who will replace an air bag wire in the steering wheel. The wire can become chafed, causing a short circuit that can lead to the airbag inflating unexpectedly. Ford said it knows of no crashes caused by the problem. But NHTSA said in a January letter to Ford the agency knew of 269 cases where the air bags deployed inadvertently, resulting in 98 injuries, some serious. Source:

<http://www.msnbc.msn.com/id/42587899/ns/business-autos/>

DEFENSE/ INDUSTRY BASE SECTOR

Ill. man denies taking military data to China. An Illinois man accused of taking restricted military data to China has pleaded not guilty. An attorney for the man entered the plea April 14 in federal court in Newark, New Jersey. He was originally granted bail in Illinois, but was later ordered held on \$750,000 bail by a judge in New Jersey. He is accused of taking documents from his job at L3 Communications in New Jersey to China, where he was speaking at a technology conference last November. He faces one count of exporting defense-related data without a license, a charge that carries a possible 20-year prison sentence. The man's attorney said her client is a legal permanent resident of the United States but is being targeted because of his Chinese heritage. Source:

<http://www.militarytimes.com/news/2011/04/ap-illinois-man-denies-taking-military-data-to-china-041411/>

EMERGENCY SERVICES

Feds: No vests, no grant money. The U.S. Justice Department (DOJ) is threatening to withhold millions of dollars in federal aid to local police departments unless they adopt policies that require uniformed officers to wear body armor. The requirement, which takes effect this month as local agencies apply for as much as \$37 million in federal aid to purchase bullet-resistant vests, comes in

the wake of a recent surge in fatal shootings of police officers. The acting director of DOJ's Bureau of Justice Assistance, said the new policy is in response to the spike in violence — a 44 percent jump in fatal police shootings over the same time last year — and research showing many police agencies do not require officers to wear body armor. Last year, DOJ distributed \$37 million to reimburse 4,127 agencies for the purchase of 193,259 vests. DOJ officials began contemplating changes to the program after a 2009 review by the Police Executive Research Forum, a law enforcement think tank, found 41 percent of departments do not require officers to wear body armor at least some of the time. The federal program would mandate that officers wear the vests while in uniform. Source: <http://officer.com/online/article.jsp?siteSection=1&id=57778>

ENERGY

NSA boss anxious about e-grid safety. The director of the National Security Agency suggested American electric companies may not be able to protect the power grid in the United States from a cyberattack. "When you look at it, if you were to ask me to rank order where industries are in terms of their cybersecurity capability, I think power is at or close to the bottom of the list, not because they're bad, but because that's not a focus area for them right now," said the four-star Army general who also commands the U.S. Cyber Command. At a cybersecurity symposium April 11 at the University of Rhode Island, the general spoke of an August 2003 electrical blackout that affected 45 million people in 8 Eastern states and 10 million others in Ontario, Canada, aggravated by a software problem that was initially unknown to the systems operators. He also addressed an August 2009 sensing-system failure at the world's third largest hydroelectric plant at the Sayano-Shushenskaya dam in Russia, where engineers remotely turned on a turbine that violently tore apart, causing a ceiling to collapse at the power plant, damaging eight other turbines and killing 75 people. "What I'm concerned about: these are issues that were caused by people with good intentions," the general said. Source: http://www.govinfosecurity.com/articles.php?art_id=3533

FOOD AND AGRICULTURE

Study: U.S. meat, poultry widely contaminated with antibiotic-resistant bacteria. A recent study of the U.S. meat and poultry industry found unexpectedly high rates of bacterial contamination in products from grocery stores. Researchers with the Translational Genomics Research Institute said they found that almost half of the meat and poultry they sampled was contaminated with *Staphylococcus aureus* bacteria, 52 percent of which were resistant to at least three classes of antibiotics. In a statement, the researchers said their study was the first national assessment of antibiotic-resistant *S. aureus* in the national food supply. DNA testing suggests the animals themselves were the major source of contamination. The researchers collected 136 samples of beef, chicken, pork, and turkey from 26 retail grocery stores in Los Angeles, Chicago, Fort Lauderdale, Flagstaff, and Washington, D.C. The researchers said the fact that so many animals are infected with the bacteria suggests they are becoming immune to the steady amounts of antibiotics fed to them before slaughter. Source: <http://gantdaily.com/2011/04/15/study-u-s-meat-poultry-widely-contaminated-with-antibiotic-resistant-bacteria/>

NOAA: Gulf seafood safe to eat. A National Oceanic and Atmospheric Administration (NOAA) Fisheries chief told reporters April 12 that "not one piece of tainted seafood has entered the market"

UNCLASSIFIED

related to the 2010 BP oil spill in the Gulf of Mexico, starting within days of the well blow out. The April 20 explosion killed 11 men working on an oil platform, and resulted in the largest accidental marine oil spill in the history of the petroleum industry. The assistant administrator lead a tour of the testing labs in Pascagoula, Mississippi, to show national and regional media the rigorous methods used to insure Gulf seafood is safe — smell tests and chemical analysis. With the BP oil spill anniversary near, he said the unequivocal results are that any traces of oil in more than 40 species of marine life is 100 to 1,000 times below the level of concern, the level being set by a team of scientist from the U.S. Food and Drug Administration, NOAA, the U.S. Environmental Protection Agency, and all five Gulf states. Source: <http://www.sacbee.com/2011/04/12/3547776/noaa-gulf-seafood-safe-to-eat.html>

Salmonella in water frogs sickens 217, mostly kids. At least 217 people, mostly young children, have been sickened by salmonella spread by pet African dwarf water frogs, government health officials said. A single California breeder of the frogs has been identified as the source of infections caused by Salmonella Typhimurium confirmed in 41 states since April 2009, the Centers for Disease Control and Prevention (CDC) reported April 7. Investigators visited the breeder in March and confirmed the presence of salmonella in the environment; tests are continuing to see if it matches the outbreak strain. Infections have been detected in people from ages less than 1 to 73; the median age of infection is 5. More than 70 percent of patients have been younger than 10, officials said, and about a third of those who became ill were hospitalized. No deaths have been reported. In interviews, ill people reported contact with the frogs in the days before they became sick. Of those who could identify the type of frog, 84 percent cited African dwarf frogs, CDC said. The median time from acquiring a frog to becoming ill was 15 days, with a range of a week to eight months. The breeding center in California was first identified as the source of infections in people in 2010, CDC officials said. Children younger than 5 are among those at highest risk for salmonella infections and CDC officials warn that water frogs are not appropriate pets for kids that young. Source: http://www.msnbc.msn.com/id/42495445/ns/health-infectious_diseases/

More than 100 food recalls during first quarter. There were more than 100 food recalls during the just-ended first quarter of 2011, according to federal food safety agencies. At least 48 of the 103 recalls — almost half the total — were because manufacturers had used but failed to declare some form of allergens — ingredients such as egg, wheat, nuts, or milk. Four days into the year, the U.S. President signed the FDA Food Safety and Modernization Act (FSMA), which gives the agency the authority to force food companies to recall suspect products. But only voluntary recalls have occurred since the FSMA became law. For the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS), the first quarter saw three recalls for the dangerous E. coli O157:H7 pathogen most associated with beef cattle. Those three recalls of meat managed by FSIS totaled only 40,328 pounds. Source: <http://www.foodsafetynews.com/2011/04/more-than-100-recalls-recorded-during-1st-quarter/>

U.S. corn reserves expected to shrink to tightest level ever. U.S. corn supplies by late in the summer of 2011 are expected to shrink to the tightest levels on record amid robust demand from ethanol distillers, livestock feeders, and overseas buyers, analysts said. At the end of the 2010-11 marketing year August 31, corn stocks are expected to fall to 595 million bushels, based on the average analyst estimate in a Dow Jones Newswires survey of analysts before the U.S. Department of Agriculture's (USDA) monthly Supply and Demand report April 8. Previously, the USDA estimated 2010-11 ending

UNCLASSIFIED

UNCLASSIFIED

corn stocks at 675 million bushels, which already would be the lowest in 15 years and less than half the supplies on hand at the close of 2009-10. “Clearly, corn demand needs to be rationed,” an analyst with CattleHedging.com wrote in a report the week of April 4. “While a setback is possible at any time, the corn market seems poised to set historic highs.” If the USDA cuts projected corn reserves below 600 million bushels as expected, it would leave stocks as a percentage of use — a key indicator of the country’s supply cushion — at around 4 percent, a record low. The current low, 5 percent, was set in 1995-96. Source: <http://www.dairyherd.com/dairy-news/latest/US-corn-supply-expected-to-shrink-to-tightest-level-ever-119424719.html?ref=719>

(Rhode Island) Second death in Rhode Island salmonella outbreak. The Rhode Island outbreak of Salmonella linked to contaminated pastries has claimed a second victim. A man in his 90s, who had been hospitalized and had tested positive for the outbreak strain of Salmonella, died April 7, according to a report in the Providence Journal. The Rhode Island Department of Health said the man had eaten pastry prepared by DeFusco’s Bakery in Johnston, which closed its doors March 25 after recalling zeppole, an Italian pastry, and other baked goods. As of April 8, the health department said there have been 66 illnesses associated with the outbreak. Twenty-eight of those sickened were so ill they required hospitalization; four remain in the hospital. A man in his 80s died March 23. Health inspectors found multiple food-safety violations at the bakery, including pastry filling stored on the floor at room temperature and cardboard cartons, which previously held eggs, used to hold baked pastry shells. Lab tests later detected Salmonella in the boxes, leading to speculation that egg residue from tainted eggs may have contaminated the pastries. Source: <http://www.foodsafetynews.com/2011/04/second-death-in-rhode-island-salmonella-outbreak/>

Tainted milk case in China deemed intentional poisoning. Intentional poisoning was behind the tainted milk that killed 3 children and caused 36 others to become ill in China’s northwestern Gansu province the week of April 4, state media reported April 10, adding to the woes of the country’s maligned dairy industry. Local investigators in Pingliang city said they had arrested suspects in connection with the nitrate-laden milk that caused 39 people to seek hospital care April 7, Xinhua news agency said. It did not give details on the suspects’ identities or motives. Nitrate, which is used to cure meat, has no use as a milk additive, the official China Daily newspaper cited a health bureau official as saying. The three children who died after consuming the tainted milk were all under 2-years-old. As of April 10, 17 of the victims were hospitalized in stable condition. Source: <http://www.foxnews.com/health/2011/04/11/tainted-milk-case-china-deemed-intentional-poisoning/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(California) Chinese national charged with running scam U.S. Army unit. A Chinese national was arrested April 12 in California on charges he created a fake Army special forces unit and convinced more than 100 other Chinese nationals to join and pay him fees to participate, the Los Angeles County District Attorney’s (DA) office said. The 51-year-old suspect of El Monte, California, allegedly called himself the “Supreme Commander” of a phony military unit called the “U.S. Army/Military Special Forces Reserve.” According to the DA, he formed the unit in October 2008, and recruited other Chinese nationals by telling them joining was a path to U.S. citizenship. Members allegedly paid

UNCLASSIFIED

the man initiation fees ranging from \$300 to \$450, along with yearly \$120 renewal fees. In return, the man provided recruits with fake U.S. Army uniforms, fake documents, and fake military ID cards. He also allegedly decorated his Temple City, California office to look like a U.S. military recruiting center, and ordered his recruits to report for military training and indoctrination. The DA's office press release said the fake unit even marched in a parade in Monterey Park, and went in uniform for a tour of the USS Midway museum in San Diego. According to the Los Angeles Times, the suspect's recruits were "typically" low-wage workers at Chinese restaurants, and while most were from the Los Angeles area, some lived as far away as Georgia. An FBI spokeswoman said investigations began 3 years ago, when police began to notice some people pulling out fake military identification during traffic stops. Source:

http://tpmmuckraker.talkingpointsmemo.com/2011/04/chinese_national_charged_with_running_scam_us_army.php

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Skype for Android has a major security flaw. A major security flaw has been discovered in the Skype for Android app, which could put users' private data in danger of being accessed by others. After discovering that a leaked beta version of the VoIP app was vulnerable to an exploit that offers access to all user data, Android Police tried the same tactic with Skype for Android, available since October 2010, and saw the same results. The site notes the Skype Mobile for Verizon app appears to be unaffected, only Skype for Android. Skype stores all user data in a folder bearing that user's name. The database files contained in that folder have incorrect permissions that are not encrypted. Therefore, these files, which contain everything from contacts and profile information to message logs, can be accessed and read by anyone with minimal trouble. However, potential intruders would require a user's Skype name to access the private data. Android Police notes there is the danger of a rogue developer releasing a modified version of the app that could pull out and transmit private user information. Source: <http://www.digitaltrends.com/mobile/software-mobile/skype-for-android-has-a-major-security-flaw/>

Feds take 'Coreflood Botnet': 'Zombie' army may have infected 2 Million computers, stolen hundreds of millions of dollars. The FBI and the U.S. Justice Department (DOJ) said April 13 they have disabled a "botnet" of more than 2 million computers infected with malicious code that Eastern European cyber criminals may have used to drain millions of dollars from bank accounts around the world. U.S. authorities continue to combat the network of remotely controlled computers called the "Coreflood" botnet, which has secretly recorded computer users' keystrokes to compromise vast amounts of banking and financial data. Coreflood is believed to have been operating since 2002 and has resulted in an unknown number of U.S. bank accounts being broken into with losses that could be in the hundreds of millions of dollars, according to FBI officials. DOJ and the FBI filed a civil complaint against 13 "John Doe" defendants, charging them with wire fraud, bank fraud, and illegal interception of electronic communications. The FBI and DOJ also have executed search warrants to seize Internet domain names believed tied to the control servers for the Coreflood program. Investigators received a temporary restraining order allowing them to seize control of the infected servers to try to further dismantle and disable the botnet. Source: <http://abcnews.go.com/Technology/feds-crush-coreflood-botnet-infected-million-computers-stole/story?id=13369529>

Yahoo! allows users to monitor account login activity. Yahoo! has introduced a new feature that allows users to review their account's log-in history for strange activity and signs of possible compromise. E-mail accounts are valuable for cyber criminals and can be compromised in a variety of ways, including via keyloggers or phishing. Since storage space is no longer a major issue, a lot of people fail to delete old e-mails. This is a security risk because those messages can contain passwords and sensitive information about other accounts. Besides the more traditional illegal activities such as spamming, compromised accounts can be used to send scam e-mails to the user's own contacts, increasing the chances of finding someone willing to pay. The new feature is not limited to e-mail and covers all services provided under the same Yahoo! ID. The "Recent Login Activity" page lists logins by date, location, access client (browser, Y! Messenger), and the place of origin (Front Page, Mail, etc.). This information is used to establish a pattern, and if one login does not fit into it the entry is marked with an alert icon. The feature helps users take corrective action, such as changing their passwords, as quickly as possible in case of compromise. Source: <http://news.softpedia.com/news/Yahoo-Allows-Users-to-Monitor-Account-Login-Activity-194784.shtml>

Holes found in majority of leading network firewalls. As a new generation of firewall technology is taking hold, NSS Labs has begun testing traditional network firewalls and so-called next generation firewalls. NSS Labs engineers have discovered serious flaws in these products, despite the maturity of the market and their certification by two other major certification bodies. Researchers have found that three out of six firewall products failed to remain operational when subjected to stability tests. This lack of resiliency is troublesome, especially considering the tested firewalls were ICSA Labs and Common Criteria certified. Also, five out of six vendors failed to correctly handle the TCP Split Handshake spoof (Sneak ACK attack), thus allowing an attacker to bypass the firewall. Lastly, measuring performance based upon RFC-2544 (UDP) does not provide an accurate representation of how the firewall will perform in live real-world environments. "IT organizations worldwide have relied on third-party testing and been misled," said the CTO of NSS Labs. "These test results point towards the need for a much higher level of continuous testing of network firewalls to ensure they are delivering appropriate security and reliability." Source: <http://www.net-security.org/secworld.php?id=10882>

Email malware jumps 400% after Rustock takedown. Malware sent via e-mail increased by 400 percent in the last week of March 2011, Commtouch reported April 12. The significant increase was detected 2 weeks after the takedown of the Rustock botnet had resulted in a 30 percent drop in spam levels. While overall spam activity dropped around the New Year, it rose significantly after the holiday period. From January to mid-March, spam averaged 168 billion e-mails per day until Rustock was eliminated, dropping spam to an average of nearly 119 billion messages daily. Zombie activity also dropped significantly after Rustock was taken down, but large increases of enslaved computers became evident following the malware outbreak at the end of the quarter. The report also describes attempts by spammers and phishers to save money by hiding their online presence in disused forums or making use of online form-filling services to ease the collection of phished user data. Source: http://www.net-security.org/malware_news.php?id=1692

Privacy violations by popular mobile apps under investigation. An ongoing grand-jury investigation has revealed that many mobile applications could be sending user information to advertising

UNCLASSIFIED

networks without the users' knowledge and permission. The investigation was prompted by a report published by the Wall Street Journal last December, which presented the result of an analysis of 101 applications for the iPhone and Android-powered mobile phones: 56 transmitted the devices' unique identifiers, 47 relayed the phone's location, 5 sent out the users' age, gender, and other personal details, and 45 did not even offer a privacy policy. According to the Wall Street Journal, Pandora Media — the owner of the popular online music service — has admitted to having been served a subpoena related to the investigation. The Journal's own testing found the iPhone and Android versions of Pandora's app send out all of the data mentioned in the preceding list. The company claims they have been told the subpoena has been issued "on an industry-wide basis to the publishers of numerous other smartphone applications" and that Pandora was not "a specific target." The Journal contacted other creators and/or owners of popular apps and asked them if they had received the same subpoena. Some confirmed, others denied, and others declined to comment. Threatpost reported research by security firm Veracode confirmed Pandora's app sent personal data, and the researchers found libraries for five different ad networks embedded in it. "The data included both the owner's GPS location, and gender, birthday, and postal code information," Threatpost said. "There was evidence that the app attempted to provide continuous location monitoring — which would tell advertisers not just where the user accessed the application from, but also allow them to track that user's movement over time." Source: <http://www.net-security.org/secworld.php?id=10868>

Uptick in rogue Facebook applications. GFI Software announced the top 10 most prevalent malware threats for the month of March 2011. GFI researchers found the Japanese tsunami, earthquake, and subsequent nuclear disasters led to a high volume of cyber attacks. "In March, we saw an apparently endless collection of scams related to the earthquake and tsunami in Japan, including fake donation Web sites, Facebook clickjacking and 419 spam e-mails (otherwise known as advance-fee frauds, where the target is fraudulently persuaded to advance sums of money). In addition, we also observed search engine poisoning involving radiation levels that sent people to malware sites," a senior threat researcher at GFI Software said. March also saw many other forms of attack, including numerous rogue Facebook applications, ransomware, and fake antivirus programs and system defragmenters. Scammers also started with SEO poisoning related to printable Easter cards and Skype calls from individuals who attempt to have their victim visit a URL that promotes a fake antivirus program. GFI statistics showed Trojans made up 7 of the top 10 malware threats of the month. Trojans detected as Trojan(dot)Win32(dot)Generic!BT (a generic detection that encompasses a broad array of trojans) continue to be the number one threat, accounting for about 20 percent of total malware found. Source: http://www.net-security.org/malware_news.php?id=1687

NATIONAL MONUMENTS AND ICONS

(Missouri) Health department warns large prescribed burns in Mark Twain National Forest could affect air quality. The Springfield-Greene County Health Department in Missouri said two large prescribed burns in the Mark Twain National Forest could affect nearby Taney and Ozark counties' air quality indexes. Crews are burning about 6,000 acres at Big Creek and Three Sisters near Ava. With no control of incoming breezes, health department warned the winds are unhealthy for anyone with heart or long disease. The agency's air quality control division expected smoke to drift in April 13 or 14. According to the health department, particulate matter may contain fine particles with microscopic solids or liquid droplets that can become embedded in the lungs and cause serious

UNCLASSIFIED

health problems. If particulate matter continues to travel into the Springfield area, air quality levels could be elevated to the "Slightly Unhealthy" or orange level. Such levels of air quality could be potentially harmful for people with heart or lung disease, older adults, and children. People who fall into these categories should avoid prolonged exposure or heavy exertion when air quality levels are elevated to "Slightly Unhealthy" or orange levels. Source: <http://www.kspr.com/news/local/kspr-health-department-warns-large-prescribed-burns-in-mark-twain-national-forest-affecting-air-quality-20110413,0,3217294.story>

POSTAL AND SHIPPING

Postal Inspectors warn of change of address scam. The U.S. Postal Inspection Service is warning consumers of a "change of address" scam they are seeing more frequently. Postal inspectors said unauthorized Web sites are not submitting a change of address after charging people a \$20 to \$30 fee. Inspectors said the U.S. Postal Service charges \$1 to change an address online, or if a person goes to the post office in person, it is free. Source: <http://www.kmov.com/news/national/Postal-Inspectors-warn-of-change-of-address-scam-119901954.html>

PUBLIC HEALTH

Shortage of leukemia drug forcing hospitals to turn some patients away. A critical shortage of a leukemia drug has cancer centers across the country worried about how to treat many of their patients. Oncologists in 30 states have reported a shortage of cytarabine, a drug that is key to treating certain types of leukemia. "If we can't get the drug, then the patients are going to die," the chairman of the Department of Leukemia at the University of Texas M.D. Anderson Cancer Center in Houston said. One of the drug's three U.S. manufacturers, Hospira, said its delays were caused when the company was unable to obtain the active ingredient, cytarabine, from its supplier. Hospira and another manufacturer, APP, also had a problem with crystallization in drug vials. APP recalled a supply in February. Bedford Laboratories said its delays are "due in part to the fact Bedford continues to face increased market share of product demand due to a decrease in competitor's capacity." Cytarabine is used as part of a drug regimen against acute myeloid leukemia (AML), a relatively rare cancer. It is sometimes used to treat acute lymphoblastic leukemia (ALL). For patients with AML who take cytarabine, the drug is the difference between a shot at life and certain death. "Since its introduction, we can claim cures in 40 to 50 percent of patients," the director said. "Without the drug in the treatment regimen, the rate is zero." Doctors said there are no suitable substitutes for cytarabine, leaving AML patients without a viable alternative. A number of hospitals said they have to ration supply, meaning some patients will not get the doses they need. It also means they must turn new patients away. Nebraska Medical Center in Omaha said, "At one point last week, we were completely out of enough cytarabine for any new patients. We had enough to finish the current patients we had in the hospital but no new ones." Source: <http://abcnews.go.com/Health/shortage-leukemia-drug-cytarabine-forcing-hospitals-turn-patients/story?id=13374817>

(Maryland) Army starts clinical trials on ricin vaccine. The U.S. Army said it is starting clinical trials at Fort Detrick in Maryland on a potential ricin vaccine. The U.S. Army Medical Research Institute of Infectious Diseases said April 13 there currently are no federally approved countermeasures to ricin. The deadly toxin derived from castor beans is considered a significant biological warfare or terrorism threat. Two civilian scientists at the Army laboratory in Frederick first reported in 2004 on a vaccine

UNCLASSIFIED

candidate they developed through molecular modeling and protein engineering. It has been proven effective in lab animals and is now being tested on 30 human volunteers. Ricin can cause respiratory failure within 72 hours when inhaled. It is also deadly when swallowed. Source:

http://www.foxbaltimore.com/template/inews_wire/wires.regional.md/2877c681-www.foxbaltimore.com.shtml

Johnson & Johnson recalls Topamax for odor. Johnson & Johnson (J&J) April 14 announced a recall of 57,000 bottles of the prescription anti-seizure medication Topamax following consumer complaints of an “uncharacteristic odor.” J&J said the recall represents two lots of the Topamax 100 mg tablets made by its Ortho-McNeil Neurologics division. The affected drugs were shipped and distributed between October 19 and December 28, 2010 in the United States and Puerto Rico. The company said it believes fewer than 6,000 bottles of the medicine remain in the marketplace to be recalled.

However, Ortho-McNeil Neurologics said it does not anticipate a product shortage resulting from the recall. J&J said it initiated the recall after receiving four consumer reports of an uncharacteristic odor thought to be caused by trace amounts of TBA (2,4,6 tribromoanisole). McNeil recalled more than 50 million bottles of Tylenol, Motrin, and Benadryl products in 2010 after receiving similar complaints of an unusual moldy, musty odor. The company said at the time the smell was caused by trace amounts of the same chemical, TBA, which is applied to wooden pallets used to transport and store packaging materials. While not considered to be toxic, J&J said TBA can generate an offensive odor, and a very small number of patients have reported temporary gastrointestinal symptoms. Source:

http://money.cnn.com/2011/04/14/news/companies/topamax_recall_johnson/?section=money_late_st

(Utah) 4 cases of measles confirmed in Granite School District. Four cases of measles were confirmed in the Granite School District in Holladay, Utah, and several schools have been affected by the outbreak. The schools affected are Olympus and Skyline high schools, William Penn Elementary, and Evergreen Jr. High. The quarantine on students who have not been immunized was extended to April 25. Now, 22 students from Olympus High and 2 students from William Penn Elementary, along with teachers who have not been immunized, must stay home until that date. The Granite School District is working to prevent the measles outbreak from spreading to more schools. State law does not require children to immunized, and they can get an exemption from health officials. But if there is an outbreak of a disease in the school, then those affected are required to stay home. About 2 to 3 percent of students in the schools have not been immunized. Source:

<http://www.fox13now.com/news/local/kstu-measles-outbreak-measles-outbreak-spreads-to-4-utah-schools-20110411,0,7189663.story>

TRANSPORTATION

Democrats press for biometric screening of flight crews. Democratic leaders of the U.S. House Homeland Security Committee pressed the administrator of the Transportation Security Administration (TSA) April 12 to ensure a biometric solution for airplane crewmember screening. The lawmakers noted such a system is authorized by the Implementing Recommendations of the 9/11 Commission Act (Public Law 110-53), which contains a provision enabling TSA to establish an “expedited security screening system for sterile area access control within commercial service airports.” TSA has been working on a crewmember identity verification system the past 3 years. The Democratic Representatives said not only does it make sense to apply the system to all

UNCLASSIFIED

UNCLASSIFIED

crewmembers, but doing so would reduce congestion at air passenger security checkpoints and enable TSA screeners to focus more effectively and efficiently on possible threats. Source:

<http://www.hstoday.us/briefings/today-s-news-analysis/single-article/democrats-press-for-biometric-screening-of-flight-crews/4722a697b3ac2f6aabb7639f48e4df06.html>

US blocks 350 suspected terrorists from planes. The U.S. government has prevented more than 350 people suspected of ties to al-Qaida and other terrorist groups from boarding U.S.-bound commercial flights since the end of 2009, the Associated Press (AP) has learned. The tighter security rules — imposed after the attempted bombing of an airliner Christmas 2009 — reveal a security threat that persisted for more than 7 years after the September 11th attacks. Until then, even as commercial passengers were forced to remove their shoes, limit the amount of shampoo in their carry-on luggage and endure pat downs, hundreds of foreigners with known or suspected ties to terrorism passed through security and successfully flew to the United States each year, U.S. officials told AP. The government said these foreigners typically told customs officers they were flying to the U.S. for legitimate reasons such as vacations or business. Security practices changed after an admitted al-Qaida operative from Nigeria was accused of trying to blow himself up on a flight to Detroit, Michigan. Until then, airlines only kept passengers off U.S.-bound planes if they were on the no-fly list, a list of people considered a threat to aviation. Now before an international flight leaves for the United States, the government checks passengers against a larger watch list that includes al-Qaida financiers and people who attended training camps but are not considered threats to planes. The government was checking this list before, but only after the flight was en route. If someone on the flight was on the watch list, the person would be questioned and likely refused entry to the country after the plane landed. The new policy has not turned the 450,000-person terror watch list into the no-fly list. Simply being on the terror watch list does not mean a person won't be allowed to enter the United States. Source: http://www.msnbc.msn.com/id/42529687/ns/us_news-security/

WATER AND DAMS

Nothing Significant to Report

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7): 866-885-8295(IN ND ONLY)**; Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**

UNCLASSIFIED

UNCLASSIFIED



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED